(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
19. September 2013 (19.09.2013)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2013/135807 A1

(51) Internationale Patentklassifikation:
G05B 19/048 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2013/055225

(22) Internationales Anmeldedatum:
14. März 2013 (14.03.2013)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2012 102 187.2 15. März 2012 (15.03.2012) DE

(71) Anmelder: **PHOENIX CONTACT GMBH & CO.KG** [DE/DE]; Flachsmarktstrasse 8, 32825 Blomberg (DE).

(72) Erfinder: **SCHMIDT, Joachim**; Waldecker Straße 37, 31812 Bad Pyrmont (DE).

(74) Anwalt: **BLUMBACH ZINNGREBE**; Alexandrastraße 5, 65187 Wiesbaden (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

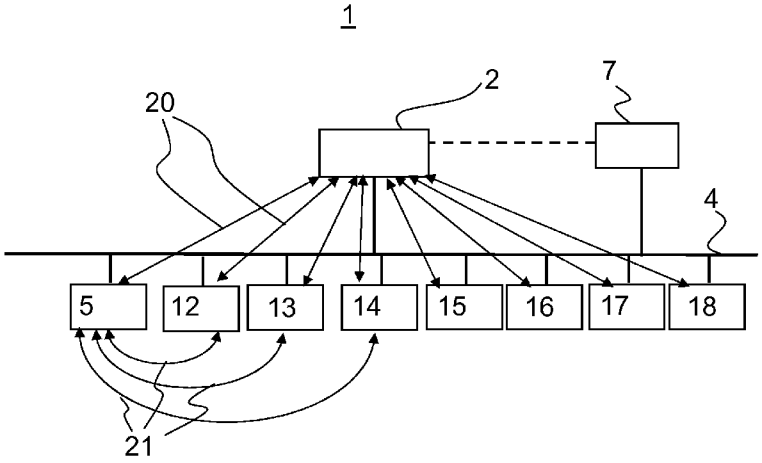
— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

[Fortsetzung auf der nächsten Seite]

(54) **Title**: CONTROL DEVICE FOR CONTROLLING SAFETY-CRITICAL PROCESSES IN AN AUTOMATED PLANT AND METHOD FOR PARAMETERIZING THE CONTROL DEVICE

(54) **Bezeichnung** : STEUERUNGSVORRICHTUNG ZUM STEUERN VON SICHERHEITSKRITISCHEN PROZESSEN IN EINER AUTOMATISIERTEN ANLAGE UND VERFAHREN ZUR PARAMETERIERUNG DER STEUERUNGSVORRICHTUNG

Fig. 1



(57) **Abstract**: The invention relates to safety-related functions in automation systems for controlling industrial production processes. The aim of the invention is to provide a simple and safe parameterization of the safety-related apparatuses of such an automation plant. After a start signal sent by the communication master is received, all further activities for parameterization are controlled by a logic module.

(57) **Zusammenfassung**: Die Erfindung betrifft sicherheitsgerichtete Funktionen in Automatisierungssystemen zur Steuerung industrieller Fertigungsprozesse. Der Erfindung liegt die Aufgabe zugrunde, eine einfache und sichere Parametrierung der sicherheitsgerichteten Einrichtungen einer solchen Automatisierungsanlage bereitzustellen. Dabei werden nach dem Empfang eines vom Kommunikationsmaster gesendeten Startsignals alle weiteren Aktivitäten zur Parametrierung von einem Logikmodul gesteuert.

WO 2013/135807 A1

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eingehen (Regel 48 Absatz 2 Buchstabe h)*

Steuerungsvorrichtung zum Steuern von sicherheitskritischen Prozessen in einer automatisierten Anlage und Verfahren zur Parametrierung der Steuerungsvorrichtung

Beschreibung

Die Erfindung betrifft allgemein das technische Gebiet der Automatisierungssysteme zur Steuerung industrieller Fertigungsprozesse. Insbesondere betrifft die Erfindung sicherheitsgerichtete Funktionen in solchen Automatisierungssystemen, sowie die Parametrierung der sicherheitsgerichteten Funktionen.

Aus der DE 10 2009 042 354 A1 sind ein Verfahren und eine Vorrichtung zur sicherheitsgerichteten Kommunikation im Kommunikationsnetzwerk einer Automatisierungsanlage bekannt. Eine grundlegende Idee besteht dabei darin, die Sicherheitsfunktion einer Anlage in kleine, überschaubare, lokal begrenzbare und einfach verifizierbare Modulgruppen aufzuteilen. Diese Gruppen bilden mehr oder weniger autarke Inseln innerhalb des Kommunikationsnetzwerks. Im Speziellen sind ein nicht sicherer Kommunikations-Master und mehrere dezentrale Module als Netzwerkteilnehmer vorgesehen. Die dezentralen Module sind dementsprechend mit dem Kommunikations-Master mittels eines Kommunikationsnetzwerkes vernetzt, wobei die Kommunikation zwischen den dezentralen Modulen im Kommunikationsnetzwerk über Telegramme realisiert wird. Dabei sind mehrere der Module Sicherheitsmodule, zwischen denen sicherheitsgerichtete Daten übermittelt werden und eine logische Gruppe von Modulen zur Ausführung einer sicherheitsgerichteten Funktion bilden. Für die Kommunikation der Sicherheitsmodule innerhalb einer logischen Gruppe hält der Kommunikations-Master eine

Routing-Tabelle, in welcher logische Verbindungen zwischen den dezentralen Sicherheitsmodulen entsprechend der sicherheitsgerichteten Funktion abgelegt sind. Der Kommunikations-Master nimmt dann gesteuert anhand der Routing-Tabelle ein automatisches Routing der Daten vom sendenden Sicherheitsmodul zum empfangenden Sicherheitsmodul vor, so dass eine Kommunikation zwischen den zu einer logischen Gruppe gehörenden Sicherheitsmodulen jeweils über zwei Punkt-zu-Punkt Verbindungen, nämlich vom sendenden Sicherheitsmodul zum Kommunikations-Master und weiter vom Kommunikations-Master zum empfangenden Sicherheitsmodul erfolgt. Das Kommunikationsnetzwerk weist eine Einrichtung auf, um Informationen für das Erstellen der Routing-Tabelle von den Sicherheitsmodulen abzufragen und die Routing-Tabelle anhand dieser Information zu erstellen.

Die DE 10 2009 042 368 A1 beschreibt weiterhin ein Steuerungssystem zum Steuern von sicherheitskritischen Prozessen mit einem nicht sicheren Kommunikations-Master und einem nicht sicheren Kommunikations-Netzwerk. Zumindest einige der Netzwerkteilnehmer umfassen Sicherheitsdateneingangs-Objekte (SDI-Objekte), wie z.B. sicherheitsgerichtete Sensoren und/oder Sicherheitsdatenausgangs-Objekte (SDO-Objekte), wie etwa sicherheitsgerichtete Aktoren. An das Netzwerk sind Netzwerkteilnehmer angeschlossen, die als dezentrale sichere Netzwerkteilnehmer ausgebildet sind und im Unterschied zu den SDI- oder SDO-Objekten jeweils eine eigene dezentrale Sicherheitssteuerung aufweisen. Dazu weisen diese Netzwerkteilnehmer eine eindeutige, einstellbare Sicherheitsadresse auf.

Die sicheren Netzwerkteilnehmer sind mit SDI- und/oder SDO-Objekten zu Sicherheitsinseln gruppiert. Mit dieser Konfiguration ist gesteuert durch die dezentralen Sicherheitssteuerung sowohl eine inselinterne Kommunikation zwischen sicherem Netzwerkteilnehmer und zugeordneten SDI- und SDO-Objekten, als auch eine inselübergreifende sicherheitsgerichtete Kommunikation zwischen den sicheren Netzwerkteilnehmern möglich.

Der Erfindung liegt nun die Aufgabe zugrunde, eine einfache und sichere Parametrierung der sicherheitsgerichteten Einrichtungen einer solchen Automatisierungsanlage, beziehungsweise eines Steuerungssystems zum Steuern von sicherheitskritischen Prozessen bereitzustellen. Insbesondere soll ein möglichst einfaches Verfahren, welches mit Hilfe von Mitteln, die möglichst jede nicht sichere Steuerung und jedes Netzwerk zur Verfügung stellen, die Parametrierung eines modularen, dezentralen und sicheren Automatisierungssystems ermöglicht werden.

Zur Parametrierung von Netzwerkteilnehmern ist der sogenannte iPar-Server der Profisafe-Spezifikation bekannt. Hierbei ist vorgesehen, dass die sicheren Netzwerkteilnehmer mit einem Rechner, wie etwa einem PC parametriert werden und diese Parametrierung dann remanent speichern und zusätzlich an den iPar-Server übertragen. Der iPar-Server ist selbst nicht sicher ausgelegt und kann zum Beispiel in eine nicht sichere Steuerung im Netzwerk integriert sein. Nach dem Power-Up läuft der sichere Netzwerkteilnehmer mit seiner gespeicherten Parametrierung

hoch. Ist der sichere Netzwerkteilnehmer defekt, so ist ein Austausch dieses Teilnehmers notwendig. Der neue sichere Teilnehmer verfügt nun nicht über die notwendige Parametrierung. Dieses meldet der Teilnehmer dem iPar-Server, der an ihn daraufhin die benötigten sicheren Parameter überträgt. Die sicheren Parameter müssen dazu eine eigene Absicherung gegen Verfälschung enthalten.

Im SafetyBridge-System, welches auch als INLINE-Safety-System bezeichnet wird und in den oben genannten Druckschriften DE 10 2009 042 354 A1 und DE 10 2009 042 368 A1 beschrieben wird, kann die Erfindung verwendet werden, um ein sicheres Logikmodul und die zugehörigen sicheren Netzwerkteilnehmer zu parametrieren. Es wird die Integration mit verschiedensten nicht sicheren Steuerungen und Netzwerken ermöglicht.

Das SafetyBridge-System beruht darauf, dass eine nicht sichere Steuerung, beziehungsweise ein nicht sicherer Kommunikationsmaster mit Hilfe von Verbindungen über ein beliebiges Netzwerk und von Kopierbefehlen den Austausch von sicheren Telegrammen mit sicheren E/A-Daten zwischen den Netzwerkteilnehmern mit sicheren Ein- und/oder Ausgängen und dem Logikmodul, welches die sicheren E/A-Daten verarbeitet und auch selber über sichere Ein- und/oder Ausgänge verfügen kann, ermöglicht. So entsteht zwischen dem Logikmodul und jedem ihm zugeordneten sicheren Netzwerkteilnehmer eine sichere Punkt- zu Punkt-Verbindung, auf der sichere Telegramme in beiden Richtungen übertragen werden. Die Erfindung ist insbesondere zur Parametrierung eines Logikmoduls dieses SafetyBridge-Systems geeignet.

Erfindungsgemäß ist eine Steuerungsvorrichtung mit einem Kommunikationsnetzwerk zum Steuern von sicherheitskritischen Prozessen in einer automatisierten Anlage, sowie ein damit durchführbares Parametrierungsverfahren vorgesehen, wobei das Kommunikationsnetzwerk

- einen insbesondere nicht sicheren Kommunikationsmaster zur Steuerung des Datenflusses auf dem Kommunikationsnetzwerk und
- eine Mehrzahl von Netzwerkteilnehmern, wobei
- zumindest eine Teilmenge der Netzwerkteilnehmern als sichere Netzwerkteilnehmer ausgebildet sind, und
- zumindest ein sicheres Logikmodul als weiteren Netzwerkteilnehmer zum Steuern einer sicherheitsrelevanten Applikation mittels einer Gruppe von sicherheitsgerichteten Netzwerkteilnehmern aufweist, wobei das Logikmodul und der Kommunikationsmaster eingerichtet sind zur Durchführung folgender Schritte, um das Logikmodul zu parametrieren:
- das Logikmodul sendet unter Ansprechen auf den Empfang eines über das Kommunikationsnetzwerk gesendeten Start-Kommandos an den Kommunikationsmaster eine Leseanforderung über das Kommunikationsnetzwerk,
- der Kommunikationsmaster sendet unter Ansprechen auf den Empfang der Leseanforderung Parametrierungsdaten an das Logikmodul.

Eine Besonderheit der Erfindung ist demgemäß, dass nach dem Empfang eines vom Kommunikationsmaster gesendeten Startsignals alle weiteren Aktivitäten von Empfänger, also dem Logikmodul gesteuert werden.

Die Erfindung wird nachfolgend genauer anhand von Ausführungsbeispielen und unter Bezugnahme auf die beigeschlossenen Zeichnungen näher erläutert. Dabei verweisen in den Zeichnungen gleiche Bezugszeichen auf gleiche oder entsprechende Elemente. Es zeigen:

Fig. 1 ein Verschaltungsschema einer Steuerungsvorrichtung,

Fig. 2 ein E/A-Abbild des Kommunikationsmasters,

Fig. 3 ein Ablaufdiagramm für die Parametrierung eines Logikmoduls, und

Fig. 4 eine Variante des Verschaltungsschemas mit mehreren Logikmodulen.

Fig. 1 zeigt ein Verschaltungsschema eines Ausführungsbeispiels einer erfindungsgemäßen Steuerungsvorrichtung 1 mit einem Kommunikationsnetzwerk 4, die neben der Steuerung automatischer Fertigungs- und Überwachungsprozessen auch zum Steuern von sicherheitskritischen Prozessen in einer automatisierten Anlage ausgelegt ist. Mit dem Kommunikationsmaster 2 sind eine Anzahl von Netzwerkteilnehmern 5, 12 - 18 über das Kommunikationsnetzwerk 4 verschaltet. Die Kommunikation der Netzwerkteilnehmer 5, 12 - 18 erfolgt in Weiterbildung der Erfindung über Punkt-zu-Punkt-Verbindungen mit dem Kommunikationsmaster 2. Durch ein entsprechendes Routen der Kommunikationtelegramme stellt der Kommunikationsmaster 2 dabei logische Verbindungen zwischen den Netzwerkteilnehmern 5, 12 - 18 her. In Fig. 1 sind einige

der logischen Verbindungen 21 beispielhaft eingezeichnet. Der Kommunikationsmaster 2 dient mithin zur Steuerung des Datenflusses auf dem Kommunikationsnetzwerk 4.

Obwohl die Steuerungsvorrichtung 1 zur Steuerung sicherheitskritischer Prozesse, wie etwa eine Not-Aus-Funktion einer Maschine bei einer Auslösung einer Lichtschranke verwendet wird, muss der Kommunikationsmaster 2 selbst nicht sicher ausgelegt sein.

Bei dem in Fig. 1 gezeigten Beispiel ist eine Teilmenge der Netzwerkteilnehmern 12, 13, 14, 15, 16, 17, 18, nämlich die Netzwerkteilnehmer 12, 13, 14 als sichere Netzwerkteilnehmer 12, 13, 14 ausgebildet. Das sichere Logikmodul 5 stellt ebenfalls einen sicheren Netzwerkteilnehmer dar. Im Betrieb kommuniziert das Logikmodul 5 über die Punkt-zu-Punkt-Verbindungen 20 und damit über die logischen Verbindungen 21 mit den sicheren Netzwerkteilnehmern 12, 13, 14, um einen sicherheitskritischen Prozess zu steuern. Die sicheren Netzwerkteilnehmer 12, 13, 14 können dabei insbesondere Ein- und/oder Ausgabemodule, wie Sensoren und Aktoren für den sicherheitskritischen Prozess sein.

Das SafetyBridge-System, welches dem in Fig. 1 gezeigten Ausführungsbeispiel vorzugsweise zugrunde liegt, beruht darauf, dass eine nicht sichere Steuerung, also der nicht sichere Kommunikationsmaster 2 mit Hilfe von Verbindungen über ein beliebiges Kommunikationsnetzwerk 4 und mit Kopierbefehlen den Austausch von sicheren Telegrammen mit sicheren E/A-Daten zwischen den Netzwerkteilnehmern mit sicheren Ein- und/oder Ausgängen und dem Logikmodul 5,

welches die sicheren E/A-Daten verarbeitet und auch selber über sichere Ein- und/oder Ausgänge verfügen kann, ermöglicht. So entsteht zwischen dem Logikmodul 5 und jedem ihm zugeordneten sicheren Netzwerkteilnehmer eine sichere Punkt-zu Punkt-Verbindung in Gestalt der logischen Verbindung 21, auf der sichere Telegramme in beiden Richtungen übertragen werden.

Durch die logischen Verbindungen werden die Netzwerkteilnehmer 12, 13, 14 mit dem Logikmodul zu einer Gruppe von sicherheitsgerichteten Netzwerkteilnehmern zum Steuern einer sicherheitsrelevanten Applikation verknüpft.

Um nun das Logikmodul 5 und damit auch die sicherheitsrelevante Applikation zu parametrieren, sendet das Logikmodul 5 unter Ansprechen auf ein über das Kommunikationsnetzwerk 4 empfangenes Start-Kommando an den Kommunikationsmaster 2 eine Leseanforderung.

Insbesondere ist es dabei von Vorteil, wenn der Kommunikationsmaster 2 eingerichtet ist, über das Kommunikationsnetzwerk 4 an das Logikmodul 5 das Start-Kommando zu senden, um den Vorgang des Parametrierens zu starten. Damit kann der Vorgang des Parametrierens in einfacher Weise für ein oder mehrere solcher Logikmodule bei einem Power-Up des Systems gestartet werden.

Der Kommunikationsmaster 2 ist weiterhin eingerichtet, unter Ansprechen auf den Empfang der Leseanforderung Parametrierungsdaten an das Logikmodul 5 zu senden.

Zur Übertragung der Parameterdaten werden in Weiterbildung der Erfindung nun zusätzliche nicht sichere Ein- und Ausgangs-Bytes auf dem Logikmodul 5 implementiert, über die mit Hilfe eines einfachen Parametrier-Protokolls die Parametrierungsdaten von der nicht sicheren Steuerung, beziehungsweise dem Kommunikations-Master 2 an das Logikmodul 5 übertragen werden. Dazu kann der Kommunikationsmaster 4 insbesondere eingerichtet sein, die Parametrierungsdaten in einem dafür vorgesehenen logischen Kanal zu übertragen, welcher durch einen vorbestimmten Datenbereich der über das Kommunikationsnetzwerk 4 versendeten Telegramme repräsentiert wird. Bei dem in Fig. 2 gezeigten Beispiel ist als logischer Kanal ein Parameterkanal 40 vorgesehen.

Die Parametrierungsdaten können insbesondere die Typen der über die jeweiligen Punkt-zu-Punkt-Verbindungen 20, beziehungsweise entsprechend der logischen Verbindungen 21 mit dem Logikmodul 5 verbundenen Netzwerkteilnehmer 12, 13, 14, sowie die Verknüpfungen der Netzwerkteilnehmer 12, 13, 14 untereinander, damit also die Art und Weise, wie der sicherheitskritische Prozess gesteuert werden soll, enthalten.

Gemäß einer Weiterbildung der Erfindung werden die Parametrierungsdaten mit Hilfe einer sicheren Parametrier- / Programmier-Software erzeugt, welche beispielsweise auf einem Rechner läuft. Vorzugsweise werden die Parameterdaten zumindest teilweise aus Gerätebeschreibungsdateien des Logikmoduls und der sicheren E/A-Netzwerkteilnehmer aufgebaut. Bei dem in Fig. 1 gezeigten Beispiel ist dazu ein Rechner 7, wie beispielsweise ein PC an das

Kommunikationsnetzwerk 4 angeschlossen. Auf diesem Rechner 7 wird die sichere Parametrier- / Programmier-Software abgearbeitet und baut die Parameterdaten für die sicheren E/A-Netzwerkteilnehmer, in dem in Fig. 1 gezeigten Ausführungsbeispiel also für die Netzwerkteilnehmer 12, 13, 14 auf. Alternativ oder zusätzlich kann der Rechner 7, wie anhand der gestrichelten Verbindung in Fig. 1 symbolisiert, auch direkt an den Kommunikationsmaster 2 angeschlossen sein.

Die Parametrierungsdaten können gemäß einer vorteilhaften Ausführungsform der Erfindung in Segmente unterteilt sein und werden als Datenbaustein in der nicht sicheren Steuerung, beziehungsweise dem Kommunikationsmaster 2 hinterlegt. Der Kommunikationsmaster 2 teilt dem Logikmodul 5 mit, dass ein Datenbaustein mit Parametrierungsdaten vorhanden ist und dass das Logikmodul 5 mit diesen Daten gestartet werden soll. Erfindungsgemäß werden nun alle weiteren Aktivitäten für die Parametrierung vom Datenempfänger, also hier dem Logikmodul 5 gesteuert. Das Logikmodul 5 kennt den Aufbau der Parametrierungsdaten und überträgt
eine Datenanforderung in der Form ParameterReadRequest (Segment, Offset, Länge). Diese Anforderung wird so lange übertragen, bis die nicht sichere Steuerung mit den angeforderten Daten in der Form ParameterReadResponse(Segment, Offset, Länge, Datum, Datum) antwortet. Allgemein, ohne Beschränkung auf die Ausführungsbeispiele ist gemäß dieser Weiterbildung der Erfindung das Logikmodul 5 also eingerichtet, zu erkennen, wie viele Parametrierungsdaten anzufordern sind und so lange Leseanforderungen an den Kommunikationsmaster 2 zu

versenden, bis alle Parametrierungsdaten erhalten wurden. Weiterhin ist es dazu von Vorteil, wenn der Kommunikationsmaster 2 eingerichtet ist, die Parametrierungsdaten aufzuteilen und in mehreren Telegrammen nacheinander zu versenden. Damit entfallen Beschränkungen des Umfangs der Parametrierungsdaten. Der jeweilige Empfänger der Daten (sicheres Logikmodul oder auch sichere E/A-Netzwerkteilnehmer, wie weiter unten erläutert) senden einen Read-Request also immer so lange, bis die entsprechende Read-Response bei ihm eintrifft. Hierdurch ist die Übertragung über beliebige Netzwerke und Kombinationen von Netzwerken möglich.

Hat das Logikmodul 5 alle benötigten Parametrierungsdaten aus der nicht sicheren Steuerung ausgelesen, so startet es mit der Abarbeitung der parametrierten Verknüpfungen. Die Parametrierungsdaten, die das Logikmodul 5 aus der nicht sicheren Steuerung, beziehungsweise dem Kommunikationsmaster 2 ausgelesen hat, enthalten auch die Parameter für die zugeordneten sicheren E/A-Netzwerkteilnehmer, bei dem in Fig. 1 gezeigten Beispiel also der dem Logikmodul 5 zugeordneten sicheren Netzwerkteilnehmern 12, 13, 14.

Das Logikmodul teilt den zugeordneten sicheren E/A-Netzwerkteilnehmern 12, 13, 14 über Parameter-Kanäle seinen parametrierten Zustand mit. Darauf hin lesen die sicheren E/ANetzwerkteilnehmer, also die Netzwerkteilnehmenr 12, 13, 14 ihrerseits ihre Parameter mit Hilfe des Parametrier-Protokolls über die Parameter-Kanäle aus dem Logikmodul 5 aus.

Jedes sichere Logikmodul 5 und jeder sichere E/A-Netzwerkteilnehmer wechselt in den parametrierten Zustand und startet die Verarbeitung nachdem er alle benötigten Parametrierungsdaten gelesen hat.

Um die Parameterdaten an die E/A-Module zu übertragen, werden die E/A-Bereiche für die sicheren Telegramme um einen Parameter-Kanal 41 erweitert, über den Geräte- und Kommunikationsparameter von den Logikmodulen zu den zugeordneten sicheren E/A-Netzwerkteilnehmern übertragen werden. Demnach enthält, wie in Fig. 2 dargestellt, ein sicheres Telegramm 44 einen Datenbereich 43 für sichere Nachrichten und einen Parameterkanal 41.
Im Folgenden wird anhand des in Fig. 3 gezeigten Ablaufdiagramms ein Ausführungsbeispiel für die Parametrierung eines Logikmoduls 5 beschrieben. Die Zeitachse dieses Ablaufdiagramms läuft von oben nach unten.

Der Parametrierungsvorgang beginnt mit dem Power-ON des Systems. Der Kommunikationsmaster 2 erkennt, dass eine Parametrierung für ein Logikmodul 5, beispielsweise in Form eines Daten-Bausteins zur Verfügung steht und sendet ein Start-Kommando („Start_Command(Parameter Ready)“) an das Logikmodul 5 (Schritt 31). Gemäß einer nicht auf das Ausführungsbeispiel beschränkten Weiterbildung ist das Logikmodul 5 weiterhin eingerichtet, ausgelöst durch ein Power-ON des Systems oder allgemeiner einem Initialisieren des Logikmoduls und/oder unter Ansprechen auf ein vom Kommunikationsmaster 2 empfangenes Start-Kommando zunächst ein Telegramm mit einem Zustand des Logikmoduls als Diagnose-Meldung an den Kommunikationsmaster 2 zu senden (Schritt 32, „Diagnostic Message (Logikmodule STOP)“). Das

Initialisieren kann auch ein Anschalten des Logikmoduls 5 an das Kommunikationsnetzwerk 4 umfassen.

Bei dem in Fig. 3 gezeigten Beispiel wird nach dem Empfang der Diagnose-Meldung vom Kommunikationsmaster 2 ein Start-Kommando an das Logikmodul 5 gesendet (Schritt 33). Allgemein, ohne Beschränkung auf das spezielle dargestellte Ausführungsbeispiel kann der Kommunikationsmaster 2 dazu eingerichtet sein, so lange ein Start-Kommando an ein Logikmodul 5 zu versenden, bis der Kommunikationsmaster 2 eine Leseanforderung erhält.

Als Antwort auf „Parameter-Ready", beziehungsweise allgemein auf das Start-Kommando beginnt das Logikmodul 5 mit dem Auslesen der Parameter (Schritt 34), z. B. Segment: 1, Offset: 0, Länge: 2 (Kommando „Parameter Read Request (1. 0. 2)"). Unter Ansprechen darauf sendet der Kommunikationsmaster 2 die angeforderten Daten (Schritt 35). Diese Schritte 34, 35 werden wiederholt, bis die letzten Bytes der Parametrierungsdaten übertragen wurden.

Allgemein, ohne Beschränkung auf das spezielle in Fig. 3 dargestellte Ausführungsbeispiel ist in Weiterbildung der Erfindung also das Logikmodul 5 eingerichtet, mit der Leseanforderung eine Anforderung eines bestimmten Teils der Parametrierungsdaten zu versenden. Der Kommunikationsmaster 2 ist dann entsprechend dazu eingerichtet, auf diese Anforderung den angeforderten Teil der Parametrierungsdaten zu versenden. Die nicht sichere Steuerung, beziehungsweise der Kommunikationsmaster 2 muss zur Implementierung dieses erfindungsgemäßen Protokolls demgemäß nur über die Fähigkeit verfügen, die einzelnen Parameter-Bytes in der

Form Parameter[Adresse (Segment + Offset), Länge] zu adressieren und in den Ausgabebereich zu kopieren. Dies ist meistens der Fall und somit ist die Integration in unterschiedlichste Steuerungen möglich. Auch kann die Breite des Parametrier-Protokolls an die Breite der Konsistenzbereiche der nicht sicheren Steuerung angepasst werden. Die Abarbeitung des Protokolls ist in Fig. 2 schematisch dargestellt. Im Kommunikationsmaster 2 ist der Parametersatz 47 in Segmente 48, 49 unterteilt abgespeichert. Die verschiedenen Segmente 48, 49 sind zur Verdeutlichung unterschiedlich schraffiert dargestellt. In Fig. 2 ist der Parametersatz 47 beispielhaft nur aus zwei Segmenten 48, 49 zusammengesetzt. Selbstverständlich können aber auch mehr Segmente vorhanden sein.

Die eingangsseitig vom Kommunikationsmaster 2 empfangenen Leseanforderungen 45 werden vom Kommunikationsmaster 2 dahingehend verarbeitet, dass aus einem bestimmten, in der Leseanforderung 45 angegebenen Segment 48 des im Kommunikationsmaster 2 gespeicherten Parametersatzes 47 eine bestimmte Anzahl von Bytes 49 ausgelesen wird, deren Position im Segment 48 durch einen ebenfalls in der Leseanforderung 45 angegebenen Offset 50 bestimmt ist. Die Bytes 50 werden dann ausgangsseitig in der oben bereits erwähnten Form einer ParameterReadResponse-Nachricht 51 über den Parameterkanal 40 an das Logikmodul 5 übertragen.

Sind alle Parametrierungsdaten übertragen, führt das Logikmodul 5 gemäß noch einer Weiterbildung der Erfindung eine Konsistenzprüfung der übertragenen Daten durch und sendet daraufhin eine Diagnose-Meldung an den Kommunikationsmaster (2), Schritt 36. Bei einer

fehlerfreien Übertragung kann das Logikmodul 5 in Betrieb gehen und als Diagnose-Meldung eine entsprechende Nachricht (hier: „Diagnostic Message (Loqikmodule RUN)“) an den Kommunikationsmaster 2 senden. Im Falle eines Fehlers kann als Diagnose-Meldung eine entsprechende Fehlernachricht als Diagnose-Meldung abgesendet werden. Ein möglicher Fehler ist etwa mangelnde Konsistenz der übertragenen Daten, die beispielsweise durch einen Übertragungsfehler hervorgerufen werden kann. Eine einfache Konsistenzprüfung ist eine CRC-Prüfung der empfangenen Parametrierungsdaten durch das sichere Logikmodul 5.

Auch im laufenden Betrieb der Steuerungsvorrichtung 1 können dann in den vorgesehenen Datenbereichen der versendeten Telegramme Start-Kommandos (Schritt 37) und Diagnose-Meldungen (Schritt 38) versendet werden, die signalisieren, dass derzeit keine neuen Parametrierungsdaten durch das Logikmodul 5 abzurufen sind und/oder dass das Logikmodul 5 in Betrieb ist.

Die Erfindung kann weiterhin auch dahingehend erweitert werden, dass differenzierte Startkommandos verwendet werden.

Das übliche Startkommando signalisiert dem Logikmodul 5, dass Parameter vorhanden sind und dementsprechend die oben erläuterte Verarbeitung zur Parametrierung des Logikmoduls 5 gestartet werden soll. Wie am Ausführungsbeispiel der Fig. 3 erläutert, wird daraufhin ein vom Logikmodul 5 gesteuertes Auslesen der Parameter des kompletten Projekts aus der nicht sicheren Steuerung, beziehungsweise dem Kommunikationsmaster 2 vorgenommen. Es schließt sich eine

sichere Überprüfung auf Konsistenz (CRC, Plausibilität) an. Falls die Parametrierungsdaten fehlerfrei sind, erfolgt der Start der Verarbeitung. Anderenfalls wird vom Logikmodul 5 eine Fehlermeldung als Diagnose-Meldung generiert.

Eine weitere Möglichkeit besteht darin, dass der Kommunikationsmaster eingerichtet ist, ein Startkommando zu generieren, welches signalisiert, dass eine Parameterkennung vorhanden ist. In Weiterbildung der Erfindung kann hierbei das Logikmodul zum Auslesen der Parameterkennung (Header oder CRC) aus dem Kommunikationsmaster 2 und zum sicheren Vergleich der Parameterkennung mit remanent im Logikmodul gespeicherten Parametern eingerichtet sein. Bei positivem Vergleich der Parameterkennung mit den gespeicherten Daten startet das Logikmodul mit der Verarbeitung der Parametrierungsdaten, ansonsten wird wiederum vorzugsweise eine Fehlermeldung generiert und an den Kommunikationsmaster 2 gesendet.

Noch eine weitere Möglichkeit ist ein Startkommando, welches signalisiert, dass neue Parameter, insbesondere ein komplettes Projekt remanent im Logikmodul 5 gespeichert werden soll.

Als Bestätigung und zur Sicherheitsüberprüfung kann die Parameterkennung des alten, zuvor remanent gespeicherten Parametersatzes auf der nicht sicheren Steuerung hinterlegt werden. Die alte Parameterkennung (Header oder CRC) wird dann vom Logikmodul 5 zunächst aus der nicht sicheren Steuerung ausgelesen, das Logikmodul nimmt einen sicheren Vergleich mit den remanent

gespeicherten Parametern vor. Sind die Daten konsistent, löscht das Logikmodul 5 seinen remanenten Speicher, ansonsten sendet das Logikmodul 5 eine Fehlermeldung. Bei konsistenten Daten erfolgt ein Auslesen der neuen Parameter aus der nicht sicheren Steuerung mittels einer oder mehrerer Leseanforderungen des Logikmoduls. Die ausgelesenen neuen Parametrierungsdaten werden erneut auf Konsistenz überprüft, vorzugsweise mit CRC und einer Plausibilitätsprüfung. Falls die Parametrierungsdaten vom Logikmodul 5 als fehlerfrei erkannt werden, werden oder bleiben diese remanent gespeichert. Ansonsten wird wiederum eine Fehlermeldung gesendet.

Noch ein weiteres mögliches vom Kommunikationsmaster 2 ausgebbares Startkommando ist ein Stopp-Befehl für die Verarbeitung. Das Logikmodul kann hier eingerichtet sein, unter Ansprechen auf den Empfang dieses Startkommandos die Verarbeitung zu stoppen und entweder neu zu starten, oder es werden neue Parametrierungs-Daten angefordert.

Bei den bisher beschriebenen Ausführungsformen der Erfindung stellt der Kommunikationsmaster 2 die Datenquelle für die Parametrierungsdaten des Logikmoduls 5 dar. Es ist nun auch möglich, dass das Logikmodul 5 nach Empfang der Parametrierungsdaten seinerseits als Datenquelle fungiert. Gemäß einer ersten Ausführungsform dieser Weiterbildung der Erfindung stellt dabei das Logikmodul 5 den zugeordneten sicheren Netzwerkteilnehmern 12, 13, 14 die für diese bestimmten Parametrierungsdaten zur Verfügung.

Sobald das sichere Logikmodul alle Parameter aus der nicht sicheren Steuerung ausgelesen hat, meldet es über die Parameter-Kanäle an die zugeordneten sicheren Netzwerkteilnehmer 12, 13, 14 als Startkommando, dass Parameter für sie bereitstehen. Diese lesen darauf hin in der oben beschriebenen Weise ihre Parameter aus dem Logikmodul 5 aus. Demgemäß sind die dem Logikmodul 5 für die Steuerung einer sicherheitsgerichteten Applikation zugeordneten sicheren Netzwerkteilnehmer 12, 13, 14, oder zumindest einer dieser zugeordneten sicheren Netzwerkteilnehmer 12, 13, 14 dazu eingerichtet, unter Ansprechen auf den Empfang eines über das Kommunikationsnetzwerk 4 vom Logikmodul 5 gesendeten Start-Kommandos an das Logikmodul 5 eine Leseanforderung über das Kommunikationsnetzwerk 4. Das Logikmodul 5 ist seinerseits eingerichtet, unter Ansprechen auf den Empfang der Leseanforderung Parametrierungsdaten an den jeweiligen sicheren Netzwerkteilnehmer 12, 13, 14 zu senden, von welchem die Leseanforderung empfangen wurde.

Das Start-Kommando des sicheren Logikmoduls 5 kann also beispielsweise die Nachricht an die Netzwerk-Teilnehmer enthalten, dass Parameter vorhanden sind und die Verarbeitung gestartet werden soll. Als dadurch ausgelöste Aktionen der zugeordneten sicheren E/A-Netzwerkteilnehmer 12, 13, 14 erfolgt gemäß einer Ausführungsform der Erfindung ein Auslesen der Parameter (Kommunikations- und Geräte-Parameter) aus dem sicheren Logikmodul 5 und eine sichere Überprüfung auf Konsistenz (CRC, Plausibilität). Falls die Überprüfung fehlerfrei ist, erfolgt ein Wechsel der in den parametrierten Zustand, Start der Verarbeitung

mit Übertragung von sicheren E/A-Daten. Ansonsten erfolgt eine Fehlermeldung.

Außerdem kann ein Startkommando auch die Anweisung enthalten, dass die Verarbeitung gestoppt werden soll. In diesem Fall können die sicheren Netzwerkteilnehmer 12, 13, 14 eingerichtet sein, unter Ansprechen auf den Empfang eines solchen Startkommandos in den nicht parametrierten Zustand zu wechseln und eine Übertragung von sicheren Ersatzwerten mittels einer Leseanforderung beim Logikmodul 5 anfordern.

Die Erfindung bietet auch den Vorteil, dass sich das Verfahren zum Parametrieren hierarchisch erweitern lässt. Einem Logikmodul 5 können weitere Logikmodule als unterlagerte E/A-Teilnehmer zugeordnet sein. Die unterlagerten Logikmodule können ihre Parameter (einschließlich der Verknüpfungsanweisungen) dann aus dem überlagerten Logikmodul 5 auslesen. Für den Anwender stehen so mehr sichere E/A-Punkte und Verarbeitungskapazitäten zur Verfügung. Aus Anwendersicht gibt es nur ein System, das durch das überlagerte Logikmodul repräsentiert wird.

Das Auslesen aus dem überlagerten Logikmodul 5 kann insbesondere auf gleiche Weise geschehen, wie das oben beschriebene Auslesen der Parametrierungsdaten vom Logikmodul 5 aus dem Kommunikationsmaster 2.

Gemäß einer Weiterbildung der Erfindung sind also an das Kommunikationsnetzwerk 4 neben dem Logikmodul 5 zumindest ein weiteres Logikmodul angeschlossen, wobei das erste Logikmodul in erfindungsgemäßer Weise durch ein

Startkommando des Kommunikationsmasters, zumindest einer Leseanforderung des Logikmoduls und einer Übertragung der Parametrierungsdaten vom Kommunikationsmaster 2 zum Logikmodul 5 parametriert wird, und wobei das weitere Logikmodul in entsprechender Weise parametriert wird, indem nach Erhalt der Parametrierungsdaten das Logikmodul ein Startkommando an das weitere Logikmodul sendet, das weitere Logikmodul unter Ansprechen auf den Erhalt des Startkommandos eine Leseanforderung an das erste Logikmodul absendet und das erste Logikmodul unter Ansprechen auf den Empfang der Leseanforderung die Parametrierungsdaten an das weitere Logikmodul überträgt. Um dieses hierarchische Verfahren durchzuführen, überträgt der Kommunikationsmaster 2 zusätzlich auch die Parametrierungsdaten für das weitere Logikmodul an das erste Logikmodul 5.

Ein Ausführungsbeispiel herzu zeigt das Verschaltungsschema der Fig. 4. Neben dem Logikmodul 5 ist ein weiteres Logikmodul 51 an das Kommunikationsnetzwerk 4 angeschlossen. Das weitere Logikmodul 51 soll mit den hier als sicher ausgebildeten Netzwerkteilnehmern 16, 17 eine weitere sicherheitsgerichtete Applikation steuern. Demgemäß bilden die E/A-Netzwerkteilnehmer 16, 17 zusammen mit dem weiteren Logikmodul 51 ebenso wie die E/A-Netzwerkteilnehmer 12, 13, 14 zusammen mit dem ersten Logikmodul 5 jeweils eine logische Gruppe von Modulen zur Ausführung einer sicherheitsgerichteten Funktion. Das weitere Logikmodul 51 kommuniziert mit dem ersten Logikmodul 5 über eine logische Verbindung 22. Über diese logische Verbindung erfolgt das Absenden des Startkommandos vom ersten Logikmodul 5, die eine oder mehreren Leseanforderungen durch das weitere Logikmodul 51, sowie

die Übertragung der Parametrierungsdaten vom ersten Logikmodul 5 zum weiteren Logikmodul 51. Über die logischen Verbindungen 21, 23 können dann in einem weiteren Schritt, wie oben beschrieben, auch die jeweiligen zugeordnete E/A-Netzwerkteilnehmer 12, 13, 14, beziehungsweise 16, 17 in entsprechender Weise parametriert werden.

Generell bietet die Erfindung, wie sie oben beschrieben und in den Ansprüchen dargelegt ist, folgende Erweiterungsmöglichkeiten und Vorteile:

Die Abarbeitung des Protokolls muss nicht synchron zum Übertragungszyklus über das Netzwerk erfolgen. Konnte also das Protokoll nicht rechtzeitig zum nächsten Übertragungszyklus abgearbeitet werden, so können die alten Protokolldaten erneut gesendet werden.

Die Steuerung der Abfolge des Auslesens der Parameterdaten kann durch einen sicheren Teilnehmer so erfolgen, wie es nach den Maßgaben der Sicherheitstechnik notwendig ist. Für die Übertragung der Parameterdaten von dem sicheren Logikmodul zu sicheren E/A Netzwerkteilnehmern, wie etwa den Netzwerkteilnehmern 12, 14, 14, 16, 17 gemäß Fig. 4 und unterlagerten Logikmodulen müssen die Kopier-Routinen, die bereits für die sicheren Nachrichten vorhanden sind, wenn überhaupt, dann nur geringfügig erweitert werden. Die Kopier-Routinen, mit denen vom Kommunikationsmaster 2 die von den und an die E/A-Netzwerkteilnehmern gesendeten Daten umkopiert werden, sind in Fig. 2 symbolisch dargestellt und mit dem Bezugszeichen 52 bezeichnet.

Der Empfänger der Parameter-Daten bestimmt den Zeitpunkt der Übertragung. Hierdurch sind z.B. keine zeitgesteuerten Anfragen des Senders notwendig, ob der Empfänger bereits hochgelaufen ist oder ob die Verbindung zwischen Sender und Empfänger schon besteht. Teilsysteme laufen mit den verfügbaren E/A-Teilnehmern automatisch hoch. Später angedockte E/A-Netzwerkteilnehmer können automatisch ins System aufgenommen werden.

Es ist dem Fachmann ersichtlich, dass die Erfindung nicht auf die anhand der Figuren dargestellten Ausführungsbeispiele beschränkt ist. Vielmehr kann die Erfindung in vielfältiger Weise im Rahmen des Gegenstandes der nachfolgenden Ansprüche variiert werden. So werden bei dem in Fig.3 gezeigten Beispiel jeweils zwei Bytes von Parametrierungsdaten angefordert. Diese Länge kann jedoch an die in einem Telegramm zur Verfügung stehende Datenbreite angepasst werden. Auch kann die Anzahl der Bytes, beispielsweise durch eine entsprechende Leseanforderung während der Übertragung eines Datenbausteins von Telegramm zu Telegramm variiert werden. So sieht das Ausführungsbeispiel der Fig. 3 auch bereits vor, dass die Leseanforderung die Anzahl der angeforderten Bytes enthält.

Bezugszeichenliste:

1	Steuerungsvorrichtung
2	Kommunikationsmaster
4	Kommunikationsnetzwerk
5, 51	sicheres Logikmodul
7	Rechner
12 - 18	Netzwerkteilnehmer
20	Punkt-zu-Punkt-Verbindung
21, 22, 23	logische Verbindung
31 - 38	Verfahrensschritte zum Parametrieren des Logikmoduls 5
40, 41	Parameterkanal
43	Datenbereich für sichere Nachrichten44 sicheres Telegramm
45	Leseanforderung
47	Parametersatz
48	Segment
49	Anzahl von Bytes ausgelesen wird
50	Offset 50
51	ParameterReadResponse-Nachricht
52	Kopier-Routine

Patentansprüche

1. Steuerungsvorrichtung (1) mit einem Kommunikationsnetzwerk (4) zum Steuern von sicherheitskritischen Prozessen in einer automatisierten Anlage, wobei das Kommunikationsnetzwerk (4)
- einen insbesondere nicht sicheren Kommunikationsmaster (2) zur Steuerung des Datenflusses auf dem Kommunikationsnetzwerk (4) und
- eine Mehrzahl von Netzwerkteilnehmern (12, 13, 14, 15, 16, 17, 18), wobei
- zumindest eine Teilmenge der Netzwerkteilnehmern (12, 13, 14, 15, 16, 17, 18) als sichere Netzwerkteilnehmer (12, 13, 14) ausgebildet sind, und
- zumindest ein sicheres Logikmodul (5) als weiteren Netzwerkteilnehmer zum Steuern einer sicherheitsrelevanten Applikation mittels einer Gruppe von sicherheitsgerichteten Netzwerkteilnehmern (12, 13, 14) aufweist, wobei das Logikmodul (5) und der Kommunikationsmaster (2) eingerichtet sind zur Durchführung folgender Schritte, um das Logikmodul (5) zu parametrieren:
- das Logikmodul (5) sendet unter Ansprechen auf den Empfang eines über das Kommunikationsnetzwerk (4) gesendeten Start-Kommandos an den Kommunikationsmaster (2) eine Leseanforderung (45) über das Kommunikationsnetzwerk (4),
- der Kommunikationsmaster (2) sendet unter Ansprechen auf den Empfang der Leseanforderung (45)

Parametrierungsdaten an das Logikmodul (5).

2. Steuerungsvorrichtung (1) gemäß dem vorstehenden Anspruch, dadurch gekennzeichnet, dass das Logikmodul (5) eingerichtet ist, die Leseanforderung (45) nacheinander in Telegrammen (44) über das Kommunikationsnetzwerk (4) zumindest so lange zu verschicken, bis dieses vom Kommunikationsmaster (2) ein Telegramm (44) mit Parameterdaten erhält.

3. Steuerungsvorrichtung gemäß dem vorstehenden Anspruch, dadurch gekennzeichnet, dass das Logikmodul (5) eingerichtet ist, zu erkennen, wie viele Parametrierungsdaten anzufordern sind und so lange Leseanforderungen (45) an den Kommunikationsmaster (2) zu versenden, bis alle Parametrierungsdaten erhalten wurden.

4. Steuerungsvorrichtung (1) gemäß einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass der Kommunikationsmaster (2) eingerichtet ist, über das Kommunikationsnetzwerk (1) an das Logikmodul (5) das Start-Kommando zu senden, um den Vorgang des Parametrierens zu starten.

5. Steuerungsvorrichtung gemäß einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass der Kommunikationsmaster (4) eingerichtet ist, die Parametrierungsdaten in einem dafür vorgesehenen logischen Kanal (40) zu übertragen, welcher durch einen vorbestimmten Datenbereich der über das

Kommunikationsnetzwerk (4) versendeten Telegramme (44) repräsentiert wird.

6. Steuerungsvorrichtung gemäß einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass der Kommunikationsmaster (2) eingerichtet ist, die Parametrierungsdaten aufzuteilen und in mehreren Telegrammen nacheinander zu versenden.

7. Steuerungsvorrichtung gemäß einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass das Logikmodul 5 eingerichtet ist, ausgelöst durch ein Power-ON des Systems oder ein Initialisieren des Logikmoduls (5) und/oder unter Ansprechen auf ein vom Kommunikationsmaster 2 empfangenes Start-Kommando ein Telegramm mit einem Zustand des Logikmoduls (5) als Diagnose-Meldung an den Kommunikationsmaster (2) zu senden.

8. Steuerungsvorrichtung gemäß einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass das Logikmodul (5) eingerichtet ist, mit der Leseanforderung (45) eine Anforderung eines bestimmten Teils der Parametrierungsdaten zu versenden und der Kommunikationsmaster (2) dazu eingerichtet ist, auf diese Anforderung den angeforderten Teil der Parametrierungsdaten zu versenden.

9. Steuerungsvorrichtung gemäß einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass der Kommunikationsmaster (2) eingerichtet ist, ein

Startkommando zu generieren, welches signalisiert, dass eine Parameterkennung vorhanden ist, wobei das Logikmodul (5) zum Auslesen der Parameterkennung aus dem Kommunikationsmaster 2 und zum sicheren Vergleich der Parameterkennung mit remanent im Logikmodul gespeicherten Parametern eingerichtet ist.

10. Steuerungsvorrichtung gemäß einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass
- der Kommunikationsmaster (2) eingerichtet ist, ein Startkommando zu generieren, welches signalisiert, dass neue Parameter, insbesondere ein komplettes Projekt remanent im Logikmodul 5 gespeichert werden soll, wobei
- eine Parameterkennung des alten, zuvor remanent gespeicherten Parametersatzes im Kommunikationsmaster (2) hinterlegt ist, wobei
- das Logikmodul (5) eingerichtet ist,
- diese Parameterkennung zunächst aus dem Kommunikationsmaster auszulesen und
- einen sicheren Vergleich mit den remanent gespeicherten Parametern vorzunehmen,
- bei Konsistenz der Daten das Logikmodul (5) seinen remanenten Speicher zu löschen und
- ansonsten eine Fehlermeldung zu senden,
- bei konsistenten Daten die neuen Parameter aus dem Kommunikationsmaster (2) mittels einer oder mehrerer Leseanforderungen (45) auszulesen,
- die ausgelesenen neuen Parametrierungsdaten erneut auf Konsistenz zu überprüfen und,
- falls die Parametrierungsdaten vom Logikmodul (5)

als fehlerfrei erkannt werden, diese remanent zu speichern, und
- ansonsten eine Fehlermeldung zu senden.

11. Steuerungsvorrichtung gemäß einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass zumindest einer der dem Logikmodul (5) für die Steuerung einer sicherheitsgerichteten Applikation zugeordneten sicheren Netzwerkteilnehmer (12, 13, 14) dazu eingerichtet ist, unter Ansprechen auf den Empfang eines über das Kommunikationsnetzwerk (4) vom Logikmodul (5) gesendeten Start-Kommandos an das Logikmodul (5) eine Leseanforderung (45) über das Kommunikationsnetzwerk (4) zu senden, und wobei das Logikmodul (5) dazu eingerichtet ist, unter Ansprechen auf den Empfang der Leseanforderung (45) Parametrierungsdaten an den jeweiligen sicheren Netzwerkteilnehmer (12, 13, 14) zu senden, von welchem die Leseanforderung (45) empfangen wurde.

12. Steuerungsvorrichtung gemäß einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass
- neben einem ersten Logikmodul (5)
- zumindest ein weiteres Logikmodul (51) an das Kommunikationsnetzwerk (4) angeschlossen ist, wobei
- das erste Logikmodul (5) durch ein Startkommando des Kommunikationsmasters (2), zumindest einer Leseanforderung (45) des ersten Logikmoduls (5) und einer Übertragung der Parametrierungsdaten vom Kommunikationsmaster (2) zum ersten Logikmodul (5) parametriert wird, und wobei
- der Kommunikationsmaster (2) zusätzlich auch die

Parametrierungsdaten für das weitere Logikmodul (51) an das erste Logikmodul (5) überträgt, und wobei

- das weitere Logikmodul (51) parametriert wird, indem nach Erhalt der Parametrierungsdaten das Logikmodul (5) ein Startkommando an das weitere Logikmodul (51) sendet, das weitere Logikmodul (51) unter Ansprechen auf den Erhalt des Startkommandos eine Leseanforderung (45) an das erste Logikmodul (5) absendet und das erste Logikmodul (5) unter Ansprechen auf den Empfang der Leseanforderung (45) die Parametrierungsdaten an das weitere Logikmodul (51) überträgt.

13. Parametrierungsverfahren für eine Steuerungsvorrichtung (1) mit einem Kommunikationsnetzwerk (4) zum Steuern von sicherheitskritischen Prozessen in einer automatisierten Anlage, wobei das Kommunikationsnetzwerk (4)

- einen insbesondere nicht sicheren Kommunikationsmaster (2) zur Steuerung des Datenflusses auf dem Kommunikationsnetzwerk (4) und
- eine Mehrzahl von Netzwerkteilnehmern (12, 13, 14, 15, 16, 17, 18), wobei
- zumindest eine Teilmenge der Netzwerkteilnehmern (12, 13, 14, 15, 16, 17, 18) als sichere Netzwerkteilnehmer (12, 13, 14) ausgebildet sind, und
- zumindest ein sicheres Logikmodul (5) als weiteren Netzwerkteilnehmer zum Steuern einer sicherheitsrelevanten Applikation mittels einer

Gruppe von sicherheitsgerichteten Netzwerkteilnehmern (12, 13, 14) aufweist, wobei das Logikmodul (5) und der Kommunikationsmaster (2) folgende Schritte durchführen, um das Logikmodul (5) zu parametrieren:

- das Logikmodul (5) sendet unter Ansprechen auf den Empfang eines über das Kommunikationsnetzwerk (4) gesendeten Start-Kommandos an den Kommunikationsmaster (2) eine Leseanforderung (45) über das Kommunikationsnetzwerk (4),
- der Kommunikationsmaster (2) sendet unter Ansprechen auf den Empfang der Leseanforderung Parametrierungsdaten an das Logikmodul (5).

Fig. 1

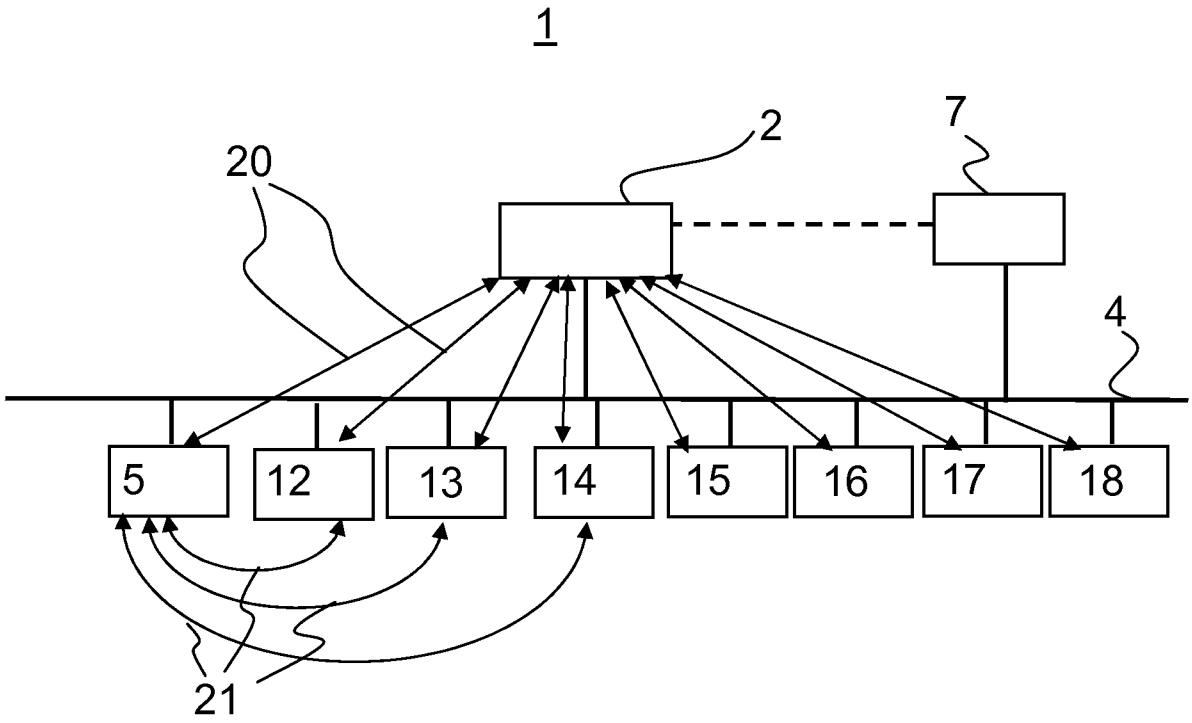
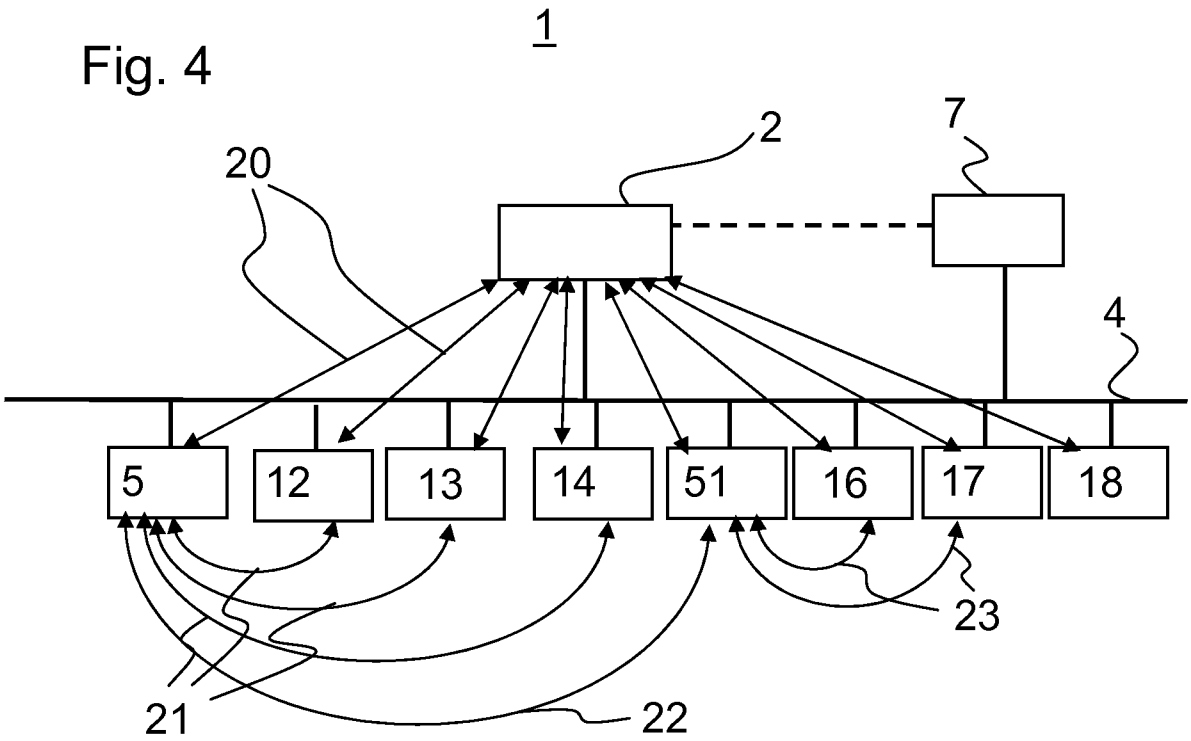

1
2
7
20
4
5
12
13
14
15
16
17
18
21

Fig. 4


1
2
7
20
4
5
12
13
14
51
16
17
18
23
21
22

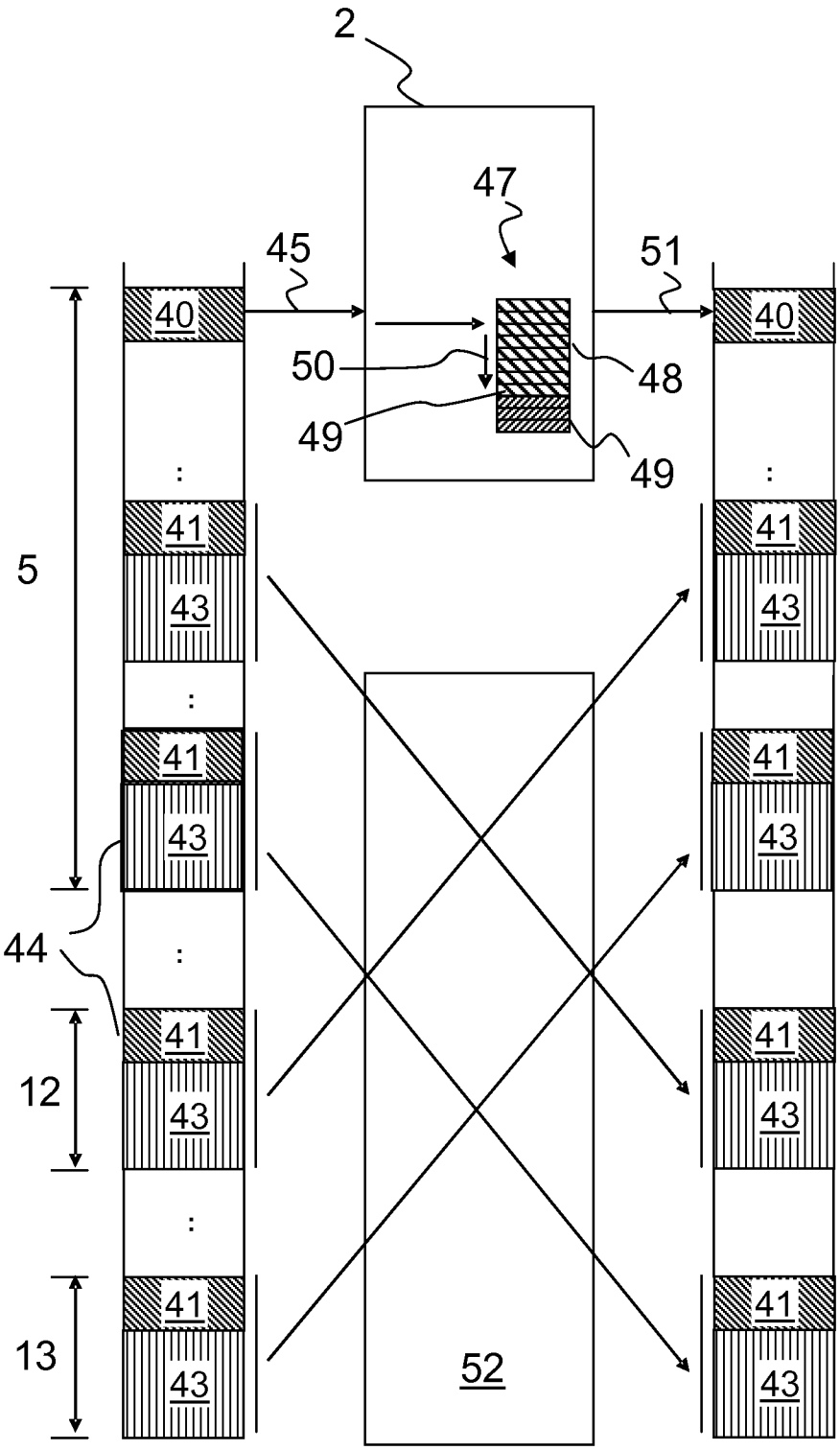

2
47
45
51
40
40
50
48
49
49
41
43
41
43
41
43
41
43
41
43
41
43
5
44
12
13
52

Fig. 2

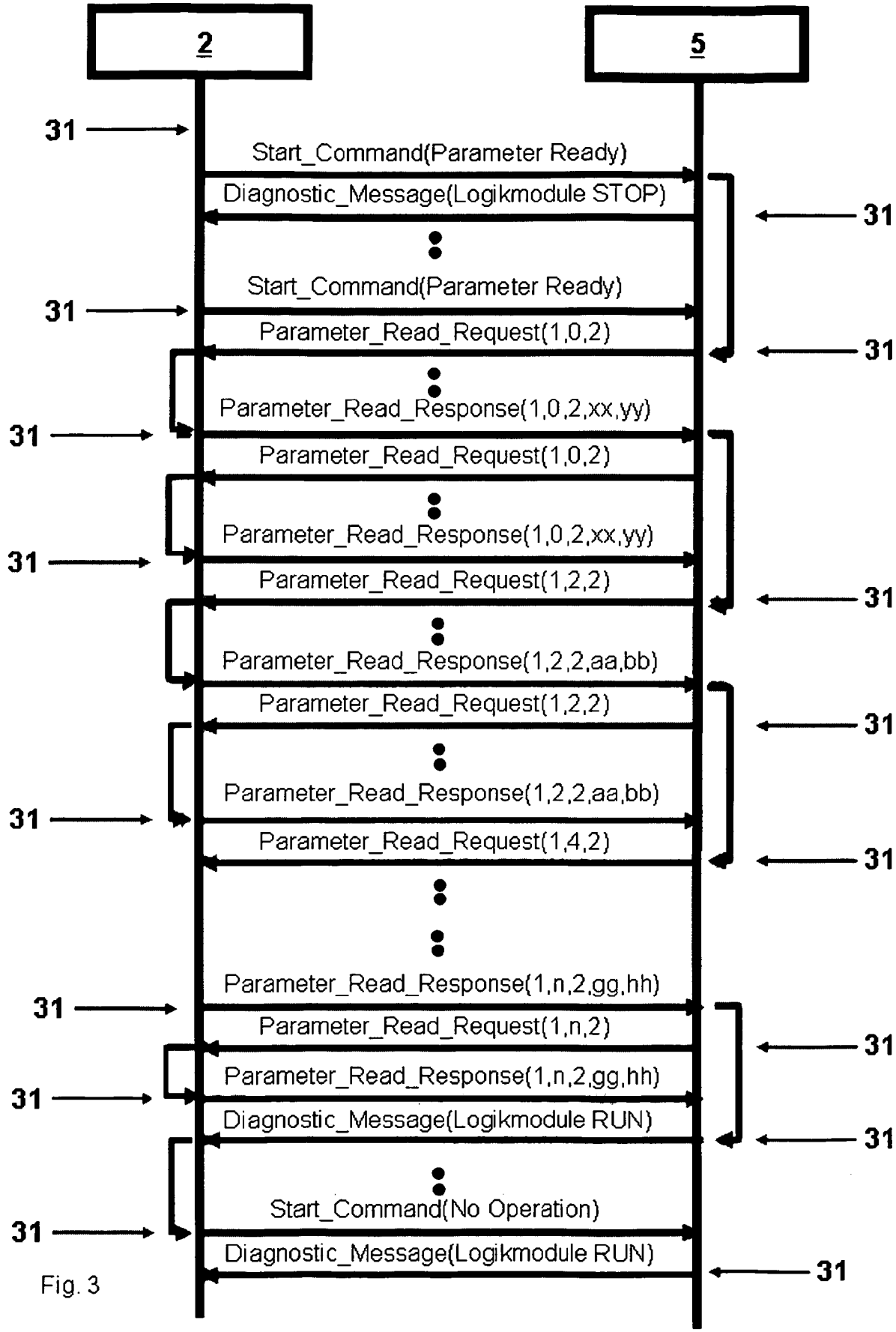

2
5
31
Start_Command(Parameter Ready)
Diagnostic_Message(Logikmodule STOP)
Start_Command(Parameter Ready)
Parameter_Read_Request(1,0,2)
Parameter_Read_Response(1,0,2,xx,yy)
Parameter_Read_Request(1,0,2)
Parameter_Read_Response(1,0,2,xx,yy)
Parameter_Read_Request(1,2,2)
Parameter_Read_Response(1,2,2,aa,bb)
Parameter_Read_Request(1,2,2)
Parameter_Read_Response(1,2,2,aa,bb)
Parameter_Read_Request(1,4,2)
Parameter_Read_Response(1,n,2,gg,hh)
Parameter_Read_Request(1,n,2)
Parameter_Read_Response(1,n,2,gg,hh)
Diagnostic_Message(Logikmodule RUN)
Start_Command(No Operation)
Diagnostic_Message(Logikmodule RUN)

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/055225

A. CLASSIFICATION OF SUBJECT MATTER
INV. G05B19/048
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 7 330 768 B2 (SCOTT CINDY [US] ET AL) 12 February 2008 (2008-02-12) figures 1,2	1-4,6-8, 11
Y	US 5 980 078 A (KRIVOSHEIN KEN D [US] ET AL) 9 November 1999 (1999-11-09) figures 11,15	1-4,6-8, 11

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 July 2013	30/07/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Sundin, Martin

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/055225

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7330768 B2	12-02-2008	CN 1542578 A	03-11-2004
		DE 102004003570 A1	10-03-2005
		GB 2399193 A	08-09-2004
		HK 1064468 A1	22-12-2006
		JP 4963779 B2	27-06-2012
		JP 2004234658 A	19-08-2004
		US 2004260408 A1	23-12-2004
US 5980078 A	09-11-1999	AU 6045498 A	08-09-1998
		AU 6045598 A	08-09-1998
		AU 6252198 A	08-09-1998
		DE 19882113 T1	27-01-2000
		DE 19882116 T5	18-11-2004
		DE 19882117 T1	27-01-2000
		GB 2336446 A	20-10-1999
		GB 2336923 A	03-11-1999
		GB 2336977 A	03-11-1999
		JP 4934482 B2	16-05-2012
		JP 2001512593 A	21-08-2001
		JP 2001512598 A	21-08-2001
		JP 2001512599 A	21-08-2001
		JP 2007226825 A	06-09-2007
		JP 2009009560 A	15-01-2009
		JP 2012084162 A	26-04-2012
		US RE40817 E1	30-06-2009
		US 5980078 A	09-11-1999
		WO 9836335 A2	20-08-1998
		WO 9836336 A1	20-08-1998
		WO 9836353 A1	20-08-1998

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2013/055225

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G05B19/048
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G05B

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	US 7 330 768 B2 (SCOTT CINDY [US] ET AL) 12. Februar 2008 (2008-02-12) Abbildungen 1,2	1-4,6-8, 11
Y	US 5 980 078 A (KRIVOSHEIN KEN D [US] ET AL) 9. November 1999 (1999-11-09) Abbildungen 11,15	1-4,6-8, 11

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
22. Juli 2013	30/07/2013

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Sundin, Martin

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2013/055225

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 7330768 B2	12-02-2008	CN 1542578 A	03-11-2004
		DE 102004003570 A1	10-03-2005
		GB 2399193 A	08-09-2004
		HK 1064468 A1	22-12-2006
		JP 4963779 B2	27-06-2012
		JP 2004234658 A	19-08-2004
		US 2004260408 A1	23-12-2004
US 5980078 A	09-11-1999	AU 6045498 A	08-09-1998
		AU 6045598 A	08-09-1998
		AU 6252198 A	08-09-1998
		DE 19882113 T1	27-01-2000
		DE 19882116 T5	18-11-2004
		DE 19882117 T1	27-01-2000
		GB 2336446 A	20-10-1999
		GB 2336923 A	03-11-1999
		GB 2336977 A	03-11-1999
		JP 4934482 B2	16-05-2012
		JP 2001512593 A	21-08-2001
		JP 2001512598 A	21-08-2001
		JP 2001512599 A	21-08-2001
		JP 2007226825 A	06-09-2007
		JP 2009009560 A	15-01-2009
		JP 2012084162 A	26-04-2012
		US RE40817 E1	30-06-2009
		US 5980078 A	09-11-1999
		WO 9836335 A2	20-08-1998
		WO 9836336 A1	20-08-1998
		WO 9836353 A1	20-08-1998